REMARKS

This Reply is in response to the Office Action of January 12, 2007 in connection with the above-identified patent application. Reconsideration of this application in view of the following remarks is respectfully requested.

Claim 3

Applicants note that the subject matter of claim 3 has been allowed. Applicants reserve the right to pursue the subject matter of claim 3 during subsequent prosecution should the present Reply not be considered to place this application in condition for allowance.

The §112 Rejections

Claims 1-4, 6-10, 12-14, 18, 21, and 24-26 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

In connection with claim 2 it was suggested that claim 2 was indefinite because the language of claim 2 does not further limit the language of claim 1. This is not correct. Claim 2 further limits the language of claim 1. Claim 1 broadly covers the use of an outer layer of message encryption to encrypt the inner-layer IBE public key. Applicants describe methods for performing an outer layer of message encryption in

their specification. For example, expressions 7 and 8 on page 40 of applicants' specification show how the outer layer of message encryption may be performed by encrypting IBE public key QG with IBE public key QL. As another example, expression 11 on page 42 of applicants' specification shows how an outer layer of message encryption may be performed by encrypting IBE public key QG with symmetric key S' and encrypting symmetric key S' with IBE public key QL. Claim 2 sets forth how the outer layer of message encryption is performed without using a symmetric key. Claim 2 therefore would not cover a situation of the type described in expression 11, which uses symmetric key S' in performing the outer layer of message encryption. Because the language of claim 2 restricts the scope of claim 1, claim 2 is not indefinite. The §112 rejection of claim 2 should therefore be withdrawn.

With respect to claims 3, 4, and 6-9, it was suggested that the language of these claims conflicts with independent claim 1, from which claims 3, 4, and 6-9 depend.

Claim 3 is directed to an arrangement of the type exemplified by expression 11. In this type of situation, the inner IBE public key QG is encrypted with a symmetric key S' (forming $QG_{S'}$) and the symmetric key S' is encrypted with the outer layer IBE public key QL (forming S'_{QL}). This type of arrangement is consistent with the embodiment of expression 11.

As mentioned above, claim 1 covers embodiments of the type shown in expression 11, so there is no contradiction between claim 3 and claim 1.

Claim 4 sets forth how the encrypted inner-layer IBE public key $QG_{S'}$ is sent to the recipient with the encrypted message $M_{S'}$. Claim 4 originally included language stating the IBE private key QL was used "to decrypt" the encrypted inner layer IBE public key. To make this clearer, the term "to decrypt" has been changed to "in decrypting." As amended, claim 4 recites how the outer-layer IBE private key QL is used in decrypting the encrypted inner-layer IBE public key $QG_{S'}$ (e.g., through use of QL in decrypting S'_{QL} as shown in the example of expression 11). The language of claim 1 encompasses embodiments of the type described in expression 11, so there is no contradiction between claim 4 and claim 1.

Claim 6 is directed towards embodiments of the type defined by expressions 8 and 11 in which the message is encrypted using a symmetric key S. Claim 1 encompasses the embodiments of expressions 8 and 11, so there is no conflict between claim 6 and claim 1. In the Office Action, it was suggested that if claim 1 requires that the message be encrypted using a public key, there would be a contradiction with claim 6 (in which the message is encrypted using a symmetric key). However, as applicants' specification makes clear (e.g., in

connection with the description of expressions 7 and 8), the message may be encrypted by encrypting message data M with symmetric key S and encrypting S with IBE public key QG (i.e., using a nested symmetric key approach) or by encrypting message data M with IBE public key QG. The language of claim 1 covers both of these possibilities, whereas the language of claim 6 narrows claim 1 to only those embodiments where message encryption includes use of a symmetric key.

Claim 7 depends from claim 6 and is directed toward arrangements in which message data M is encrypted using symmetric key S (forming M_S) and in which symmetric key S is encrypted using the inner-layer IBE public key QG (forming S_{QG}). This type of arrangement is described in connection with expression 8. Arrangements of the type defined in expression 8 are covered by claim 1, so there is no conflict between claim 7 and claim 1.

Claim 8 depends from claim 7 and is directed towards arrangements in which the process of message encryption includes encrypting the inner-layer IBE public key QG using the outer-layer IBE public key QL. An example of this type of arrangement is described in connection with expression 8. Because claim 1 covers arrangements of this type, there is no conflict between claim 8 and claim 1.

Claim 9 depends from claim 8 and is directed to

definite, not indefinite. For example, a claim limitation in which one element is said to be "longer" than another would be definite, whereas a claim limitation requiring a claim element to be "long" might be indefinite.

Moreover, key sensitivity comparisons are frequently made in the field of cryptography. For example, it is well known that the private key in a public-key/private-key pair is more sensitive than the public key. Similarly, it is well known that a master secret at a key generator is more sensitive than the private keys that are derived from that master secret. Applicants have also provided examples of keys of varying sensitivities in their specification. For example, on page 33, applicants have provided an example in which an IBE public key based on a recipient's email address is less sensitive than an IBE public key based on the recipient's security clearance.

A more extensive explanation of the implications of different key sensitivities is provided in connection with the discussion of overlapping IBE public keys on pages 43-48. As described in the example of this section of the specification, an IBE public key that is based on a validity period is less sensitive than an IBE public key that is based on an email address, the IBE public key that is based on the email address is less sensitive than an IBE public key that is based on a security clearance, the IBE public key that is based on the

security clearance is less sensitive than an IBE public key based on a rank, and the IBE public key that is based on the rank is less sensitive than an IBE public key that is based on a particularly sensitive project. By using successive layers of IBE encryption with layers that progress inwardly using more specific and sensitive IBE public keys, potentially sensitive information in the IBE public keys may be hidden from unauthorized viewing. The concept of IBE public keys of varying sensitivity is therefore well described in applicant's specification. Because key sensitivity is a well understood concept in cryptography and because applicants describe the use of keys of varying sensitivities extensively in their specification, the use of this terminology in claim 10 does not render claim 10 indefinite. Claim 10 is therefore in compliance with the requirements of §112.

In claim 13, the terms "more sensitive" and "less sensitive" to which the examiner objected are not present. Rather, claim 13 refers to data attributes that have associated "sensitivity levels." This type of arrangement is well described in applicants' specification (e.g., at page 52, lines 20-30). Examples of sensitivity levels include "none" and "high." In view of this supporting description, the term "sensitivity level" in claim 13 is not indefinite.

In claim 19, the sensitivity of the additional-layer

IBE public key is compared to that of the outer-layer IBE public key. Claim 19 is in compliance with §112 for the same reasons that claim 10 is in compliance with §112.

In claim 21, the sensitivity of the IBE public key QL is compared to that of IBE public key QG. Claim 21 is also in compliance with §112 for the reasons that claim 10 is in compliance with §112.

In claim 18, it was said that there was insufficient antecedent basis for the term "the inner layer of the message." Applicants have amended claim 18 to refer to the "inner layer of message encryption." This term is defined in claim 1, from which claim 18 depends.

Claims 24-26 were said to be unclear because of a possible conflict between claims 24-26 and base claim 21. In particular, it was suggested that the public key QG was already encrypted with symmetric key S in claim 21, leading to an inconsistency when using symmetric key S' to encrypt QG in claim 24. However, there is no inconsistency, because public key QG is not already encrypted with symmetric key S in claim 21. Rather, symmetric key S is encrypted with public key QG to produce S_{QG}. Claim 21 does not specify that public key QG is encrypted using S, so there is no inconsistency with the language of claim 24. Claim 25 depends from claim 24 and adds the feature of encrypting S' with QL to produce S'_{QL}. Claim 26

depends from claim 25 and adds the feature of sending $QG_{S'}$ and S'_{QL} to the recipient. Claims 25 and 26 are both consistent with claim 21. Support for the features of claims 24-26 is provided on pages 41 and 42 of applicants' specification in connection with the description of expression 11.

The foregoing demonstrates that claims 1-4, 6-10, 12-14, 18, 21, and 24-26 are in compliance with §112. The rejections of these claims under §112 should therefore be withdrawn.

The Claim Rejections Under 35 U.S.C. §103(a)

Claims 1, 2, 4, 5, 6-9, 13, 16, 18, 21-23, and 24-28 were rejected under 35 U.S.C. §103(a) as being unpatentable over Slick in view of Boneh. Claims 10, 11, and 18-20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Slick in view of Boneh in view of Van Oorschot. Claim 17 was rejected under 35 U.S.C. §103(a) as being unpatentable over Slick in view of Boneh in view of Lord. These rejections are respectfully traversed.

Independent claim 1 is directed towards a method for using multi-layer identity-based encryption (IBE) to securely convey a message containing message data over a communications network from a sender to a recipient. As set forth in claim 1, the message is encrypted using at least two layers of IBE

encryption. An inner layer of message encryption has an associated inner-layer IBE public key and is used to encrypt the message data. An outer layer of message encryption has an associated outer-layer IBE public key and is used to encrypt the inner-layer IBE public key. After performing message encryption at the sender, a recipient decrypts the encrypted message using an outer-layer IBE private key and an inner-layer IBE private key.

Nothing like this type of arrangement is shown or suggested by the prior art. Slick describes two embodiments of a system in which documents can be sent securely to a printer. In the first embodiment, which is shown in FIG. 5A of Slick, data is encrypted by symmetric key 510. The symmetric key is encrypted using a printer public key 520 to produce a printer-key-encrypted symmetric key 511. The printer-key-encrypted symmetric key 511 is encrypted with a recipient public key 530 to produce twice-encrypted symmetric key 512. This method of encryption is different from the method of claim 1, because it does not use an outer layer of message encryption having an associated outer-layer public key to encrypt the inner-layer public key as required by claim 1.

In the second embodiment, which is shown in FIG. 5B of Slick, the printer public key 520 is used to encrypt data 581 directly, forming printer-public-key-encrypted data 582. As

shown on the right-hand side of FIG. 5B, encrypted data 582 is then encrypted using recipient public key 530 to produce twice-encrypted data 582. This method of encryption is also different from the method of claim 1, because it does not use an outer layer of message encryption having an associated outer-layer public key to encrypt the inner-layer public key as required by claim 1.

On page 4 of the Office Action, it is acknowledged that these embodiments of Slick do not disclose the invention claimed in claim 1. Nevertheless, it is suggested that somehow a combination of these embodiments would meet the limitations of claim 1. Applicants disagree. With the first embodiment, Slick computes D_S and $(S_{PR})_{RE}$, where D represents the data 501, S represents the symmetric key 510, PR represents the printer public key 520, S_{PR} represents the encrypted key 511, and $(S_{PR})_{RE}$ represents the twice-encrypted key 512. With the second embodiment, Slick computes $(D_{PR})_{RE}$. There is no way to combine the techniques of Slick's first embodiment with the techniques of Slick's second embodiment to replicate the method of claim 1. If D is encrypted to form D_S and S is encrypted to form $(S_{PR})_{RE}$ as in the first embodiment, applying the techniques of the second embodiment would produce $((D_S)_{PR})_{RE}$ and $(S_{PR})_{RE}$ If D is encrypted to form $(D_{PR})_{RE}$ as in the second embodiment, applying the techniques of the first embodiment would produce $((D_{PR})_{RE})_S$ and

$(S_{PR})_{RE}$. In either combination, there is no use of an outer layer of message encryption having an associated outer-layer public key to encrypt the inner-layer public key as required by claim 1.

The disclosure of Slick also fails to show or suggest an inner layer of message encryption that has an associated inner-layer IBE public key, an outer layer of message encryption that has an associated outer-layer IBE public key, or use of an outer layer IBE private key or inner-layer IBE private key. There is simply no disclosure in Slick of IBE public keys or IBE private keys of any kind.

Boneh, which was cited in the §103(a) rejection, discloses an identity-based-encryption algorithm, but does not make up for the deficiencies of Slick. Moreover, there is nothing in either Slick or Boneh that suggests that the Slick and Boneh references could be combined. The Office Action also makes no mention of why Slick and Boneh should be combined or why this combination would meet the limitations of claim 1.

Because Slick and Boneh fail to show or suggest the method of claim 1 in which a message is encrypted using an inner layer of message encryption that has an associated inner-layer IBE public key and that is used to encrypt the message data and using an outer layer of message encryption that has an associated outer-layer IBE public key and that is used to

encrypt the inner-layer IBE public key, claim 1 is patentable over Slick and Boneh.

Claims 2-20 depend from claim 1 and are allowable because claim 1 is allowable.

As set forth in claim 21, encryption involves performing an inner layer of IBE encryption that includes encrypting message data M using a symmetric key S to produce encrypted message data M_S. The encryption method of claim 21 also involves using an outer layer of message encryption having an associated IBE public key QL to encrypt the inner layer IBE public key QL. As described in connection with claim 1, these features are not shown or suggested by Slick and Boneh. Claim 21 is therefore allowable for the same reasons that claim 1 is allowable, as are claims 22-28, which depend from claim 21.

The foregoing shows that claims 1-28 are in condition for allowance. This application is therefore in condition for allowance. Reconsideration of the application and allowance are respectfully requested.

Respectfully submitted,

G. Victor Treyz 7/6/07

G. Victor Treyz
Reg. No. 36,294
Attorney for Applicants
Customer No. 36532